REMARKS

Claims 1-28 are pending in the present patent application. The Examiner has rejected claims 1-28. Applicant has amended claims 1, 8, 11, 18, 22 and 28. Applicant respectfully requests reconsideration of claims 1-28 in view of at least the following amendments and remarks.

I. Objections to Drawings

The Examiner states "Figure 1 should be designated by a legend such as --Prior Art—because only that which is old is illustrated."

Applicant submits informal drawings showing the changes in red. Applicant and agrees to submit formal drawings upon allowance.

II. Objections to Claim 28

The Examiner states "Claim 28 is objected to because of the following informalities: in the second line of the claim, the second "and" should read "a"."

Applicant has amended claim 28 to correct the noted informalities.

III. Rejection of Claims 1-4 and 11-14 Based on 35 U.S.C. § 102

The Examiner has rejected independent claims 1-4 and 11-14 under 35 USC 102(b) as being anticipated by Fischer (EPO 0 638 860 A2) stating:

> In lines 38-45 of column 5, Fischer talks about signing only the critical portions of a cell. The cell is made up of objects. Applicant's snapshot, which is a copy of a main memory, directly corresponds to the critical portions of the cell.

> Digital signatures are inherently verified. Subsequently, the information that the signature was authenticating is accessed.
>
> Fischer says that this cell can itself be treated as an objected in lines 20-21 of column 8. Figure 10 shows the signatures, element 122, and the critical portions, element 116, stored in a cell.
>
> Digital signatures are inherently invalidated when the data which they are supposed to authenticate is changed.

Applicant respectfully disagrees and submits that the claims, as amended are not anticipated by the Fischer reference for at least the following reasons.

A. Claim 1-4 and 11-14

Applicant has amended independent claims 1 and 11 to incorporate the notion that the term snapshot is representative of the state of a live object during a particular point of execution (See e.g., specification page 2, lines 6-71 and page 21 lines 1-5). A snapshot represents a "picture" of a live object which is changing state. Subsequent to taking the snapshot, embodiments if the claimed invention continue to execute the live object which may result in further modification to the values of the live object (See e.g., specification page 9 lines 16-20). Applicant respectfully submits that the snapshot of the claimed invention is different than the "cell" described in the Fischer reference. A cell is basically an instance of the object and the program executing the object bound into a data file. The cell is static, and does not correspond to a live object as claimed.

In order for the Fischer reference to anticipate the claimed invention under 35 U.S.C. §102(b), the reference must teach each and every element of the claimed invention. Applicant respectfully submits that because Fischer does not

describe the use of live objects, the claims, as amended, cannot be anticipated by the Fischer reference.

V. Rejection of Claims 5-7, 15-17, and 22 Based on 35 U.S.C. § 103

The Examiner has rejected claims 5-7, 15-17, and 22 under 35 USC §103(a) as being unpatentable over Fischer in view of Schneier (Applied Cryptography). The Examiner states:

> Fischer displays a system of signing only the critical objects that make up a larger object. As can be seen in figure 10 of Fischer, elements 122 and 123, the authenticating signatures and the certificate specification set, correspond to two signatures used to authenticate the critical objects. Fisher [sic] does not say anything about one of the signatures being made from the critical objects. On page 39, Schneier shows a digital signature that is made by encrypting a message-to-be-authenticated with a private key. Decryption using the corresponding public key not only retrieves the data, but also indicates that the data was encrypted by the private key's holder. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the critical objects of Fischer to generate their signatures so that the signatures could be used as proofs against data.

A. Claims 5-7, 15-16

Applicant respectfully submits that claims 5-7, 15-16 being dependent upon respective allowable base claims are also allowable for at least the foregoing reasons stated above.

B. Claim 22

Applicant respectfully disagrees that claim 22, as amended, is rendered obvious by the prior art of record. Applicant reiterates the arguments set forth above with respect to Fischer and further adds that the Schneier reference does

not render the claimed invention obvious because Schneier does not suggest the use of encryption in relation to snapshots as claimed. Accordingly, Applicant respectfully submits that claim 22 is not obvious from Fischer in view of Schneier. Both references, either alone or in combination do not teach, suggest, or describe the user a snapshots in the manner that is claimed. More specifically, neither reference describes or suggests the use of a snapshot that represents a "picture" of a live object that is changing state. Subsequent to taking the snapshot, embodiments of the claimed invention continue to execute the live object that may result in further modification to the values of the live object.

C. Claims 8-10 and 18-21

The Examiner has rejected claims 8-10 and 18-21 under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Chaplin (5315655). The Examiner states:

> Fischer displays a system of signing only the critical objects that make up a larger object. As shown by element 114 of figure 10, Fischer's system can encrypt the cells and the digital signatures. Encryption keys are inherently generated prior to encryption. Fischer does not say that the leftover unencrypted objects are deleted. Figure 7 of Chaplin clearly shows the encryption of data in part 704 and then the deletion of the unencrypted copy of the data in part 705. Chaplin also teaches decryption of data in figure 8. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to delete unencrypted copies of the critical objects after the objects had been encrypted. Unencrypted copies could otherwise be used to circumvent the protection provided by the encryption.

Applicant respectfully submits that independent claims 8 and 18, as amended, are allowable because the Fischer reference and the Chaplin reference, either alone or in combination do not utilize snapshots that represent a live object in a particular state. Accordingly, applicant respectfully requests that claims 8 and 18 be placed in condition for allowance.

Applicant respectfully submits that claims 9-10, 19-21 being dependent upon respective allowable base claims are also allowable for at least the foregoing reasons stated above.

D. Claims 23-25

The Examiner has rejected claims 23-25 under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Schneier. The Examiner states:

> Fischer in view of Schneier shows a system of signing only the critical objects that make up a larger object where the signature is made form the critical objects. Digital signatures are inherently invalidated when the data which they are supposed to authenticate is changed. In lines 40-50 of column 2, Fischer teaches the advantage of object-oriented programming, saying that it is polymorphic. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement modules that process cells as an object to reap the rewards of polymorphism. At some point this would require the snapshot and signature to be stored within the processing object.

Claims 23-25 are dependent claims. Accordingly, Applicant respectfully submits that claims 23-25 being dependent upon respective allowable base claims are also allowable for at least the foregoing reasons stated above.

E. Claims 26-28

The Examiner has rejected claims 26-28 under 35 U.S.C. 103(a) as being unpatentable over Fischer in view of Schneier as applied to claim 22 above, and further in view of Chaplin. The Examiner states:

> Fischer in view of Schneier shows a system of signing only the critical objects that make up a larger object where the signature is made from the critical objects. As shown by element 114 of figure 10, Fischer's system can encrypt the cells and the digital signatures. Encryption keys are inherently generated prior to encryption. Fischer does not say that the leftover unencrypted objects are deleted. Figure 7 of Chaplin clearly

> shows the encryption of data in part 704 and then the deletion of the unencrypted copy of the data in part 705. Chaplin also teaches decryption of data in figure 8. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to delete unencrypted copies of the critical objects after the objects had been encrypted. Unencrypted copies could otherwise be used to circumvent the protection

Applicant respectfully submits that claims 26-28 being dependent upon respective allowable base claims are also allowable for at least the foregoing reasons stated above.

CONCLUSION

For at least the foregoing reasons, Applicant respectfully submits that pending claims 1-28 are patentably distinct from the prior art of record and in condition for allowance. Applicant therefore respectfully requests that pending claims 1-28be placed in condition for allowance.

Respectfully submitted,

THE HECKER LAW GROUP

Date: December 31, 2001

By: _____
Cynthia A. Casby
Reg. No. 47,475

THE HECKER LAW GROUP
1925 Century Park East
Suite 2300
Los Angeles, California 90067
(310) 286-0377

CERTIFICATE OF MAILING

This is to certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to Assistant Commissioner for Patents, Washington, D.C. 20231 on December 31, 2001.

D. Blizzard 12-31-01

Signature: Deanna Blizzard Date: December 31, 2001

VERSION WITH MARKINGS TO SHOW CHANGES

CLAIMS

What is claimed is:

1. Method for signing an object comprising the steps of:

taking a snapshot of the object wherein the snapshot represents the object at a point of execution;

associating a signature with said snapshot;

maintaining said association between said snapshot and said signature.

2. The method of claim 1 further comprising the steps of:

verifying said signature;

constructing a new object using said snapshot, when said signature is verified.

3. The method of claim 1 further comprising the steps of:

storing said snapshot in another object;

storing said signature in said another object.

4. The method of claim 1 further comprising the steps of:

monitoring the status of said snapshot;

invalidating said signature when the status of said snapshot changes.

5. The method of claim 1 further comprising the step of creating said signature using said snapshot.

6. The method of claim 5 further comprising the step of associating a second signature with said snapshot.

7. The method of claim 6 further comprising the steps of:

verifying said second signature;

constructing a new object using said snapshot, when said second signature is verified.

8. Method for sealing an object comprising the steps of:

generating an encryption key;

taking a snapshot of the object, wherein the snapshot represents the object at a point of execution;

generating an encrypted snapshot;

deleting said snapshot.

9. The method of claim 8 further comprising the step of associating a signature with said snapshot.

10. The method of claim 9 further comprising the steps of:

verifying said signature;

constructing a new object using said snapshot, when said signature is verified.

11. An article of manufacturing comprising:

a computer usable medium having computer readable program code embodied therein for signing an object comprising:

computer readable program code configured to cause a computer to take a snapshot of the object wherein the snapshot represents the object at a point of execution;

computer readable program code configured to cause a computer to associate a signature with said snapshot;

computer readable program code configured to cause a computer to maintain said association between said snapshot and said signature.

12. The article of manufacture of claim 11 further comprising:

computer readable program code configured to cause a computer to verify said signature;

computer readable program code configured to cause a computer to construct a new object using said snapshot, when said signature is verified.

13. The article of manufacture of claim 11 further comprising:

computer readable program code configured to cause a computer to store said snapshot in another object;

computer readable program code configured to cause a computer to store said signature in said another object.

14. The article of manufacture of claim 11 further comprising:

computer readable program code configured to cause a computer to monitor the status of said snapshot;

computer readable program code configured to cause a computer to invalidate said signature when the status of said snapshot changes.

15. The article of manufacture of claim 11 further comprising computer readable program code configured to cause a computer to create said signature using said snapshot.

VERSION WITH MARKINGS TO SHOW CHANGES

16. The article of manufacture of claim 11 further comprising computer readable program code configured to cause a computer to associate a second signature with said snapshot.

17. The article of manufacture of claim 16 further comprising:

computer readable program code configured to cause a computer to verify said second signature:

computer readable program code configured to cause a computer to construct a new object using said snapshot, when said second signature is verified.

18. An article of manufacturing comprising:

a computer usable medium having computer readable program code embodied therein for sealing an object comprising:

computer readable program code configured to cause a computer to generate an encryption key;

computer readable program code configured to cause a computer to take a snapshot of the object, wherein the snapshot represents the object at a point of execution;

computer readable program code configured to cause a computer to encrypt said snapshot;

computer readable program code configured to cause a computer to delete said snapshot.

19. The article of manufacture of claim 18 further comprising computer readable program code configured to cause a computer to decrypt said encrypted snapshot.

VERSION WITH MARKINGS TO SHOW CHANGES

20. The article of manufacture of claim 18 further comprising computer readable program code configured to cause a computer to associate a signature with said snapshot.

21. The article of manufacture of claim 20 further comprising:

computer readable program code configured to cause a computer to verify said signature; and

computer readable program code configured to cause a computer to construct a new object using said snapshot, when said signature is verified.

22. A system configured to sign an object comprising:

a first module of program code executing on a computer configured to take a snapshot of an object wherein the snapshot represents the object at a point of execution;

a second module of program code executing on said computer configured to generate a signature using aid snapshot;

said first module configured to monitor the status of said snapshot, and to invalidate said signature when said snapshot is changed.

23. The system of claim 22 wherein said first and second modules are implemented as a second object.

24. The system of claim 23 wherein said snapshot and said signature are stored in said second object, said second object limiting access to said snapshot through one or more methods of said second object.

VERSION WITH MARKINGS TO SHOW CHANGES

25. The system of claim 24 wherein said one or more methods of said second object invalidate said signature when said access modifies said snapshot.

26. The system of claim 22 further comprising a sealing module comprising:

a key generation module configured to generate an encryption key;

an encryption module configured to generate an encrypted snapshot from said snapshot;

a deletion module configured to delete said snapshot.

27. The system of claim 26 wherein said second object is configured to invoke said key generation module, said encryption module and said deletion module.

28. The system of claim 27 wherein said second object is configured to verify said signature and construct ~~and~~ a new object using said snapshot when said signature is verified.